UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/687,694	10/20/2003	Matthew Murray Williamson	1509-458	2845

22879 7590 03/10/2010

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
FORT COLLINS, CO 80528

EXAMINER	
MORAN, RANDAL D	

ART UNIT	PAPER NUMBER
2435	

NOTIFICATION DATE	DELIVERY MODE
03/10/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
ipa.mail@hp.com
laura.m.clark@hp.com

Office Action Summary	Application No.	Applicant(s)	
	10/687,694	WILLIAMSON ET AL.	
	Examiner	Art Unit	
	RANDAL D. MORAN	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 November 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-43 are pending.

Below, Examiner has pointed out particular references contained in the prior art(s) of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claims, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully each reference in its entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

Applicant's arguments, see Appeal Brief, filed 11/23/2009, with respect to the rejection(s) of claim(s) 1-43 under USC 103(a) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of.

Claim Objection

Claim 42 is objected to for lack of antecedent basis. "automatically transmitting" in line 1 lacks proper antecedent basis in the claim.

Allowable Subject Matter

Claims 10-14 and 24-28 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-9, 15-23, 29-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kaashoek et al. (US 7278159), hereafter "Kaashoek." in view of Barrett et al. (US 7,032,023), hereafter "Barrett."

Considering **Claims 1 and 43,** Kaashoek discloses a method of monitoring propagation of viruses by a first host within a network of hosts (abstract), the method comprising the following steps carried out by the first host: establishing a record which is at least indicative of identities of destination hosts within the network to whom data has been sent by the first host (Fig. 4); transmitting all requests to send data; and storing in a buffer data relating to requests which identify a destination host not in the record (column 4- lines 34-53).

Kaashoek does not explicitly disclose during a first time interval, comparing (a) identities of destination hosts identified in requests to send data from the first host and (b) identities of destination hosts identified in the record.

Barrett discloses during a first time interval, comparing (a) identities of destination hosts identified in requests to send data from the first host and (b) identities of destination hosts identified in the record (column 16- lines 26-45).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Kaashoek by during a first time interval, comparing (a) identities of destination hosts identified in requests to send data from the first host and (b) identities of destination hosts identified in the record as taught by Barrett in order to prevent the sending of SPAM messages (Barrett- column 16- lines 36-40).

Considering **Claims 29, 41, and 42,** Kaashoek discloses a method of operating a first host within a network of a plurality of hosts (abstract), said method comprising the following steps carried out by a first host: monitoring creation of sockets within the first host to identify destination hosts identified therein (Fig. 4); and storing data from all sockets which identify monitored destination hosts not in the record (column 4- lines 34-53).

Kaashoek does not explicitly disclose over the course of a first time interval, comparing identities of destination hosts monitored during the first time interval with destination hosts in a record.

Barrett discloses over the course of a first time interval, comparing identities of destination hosts monitored during the first time interval with destination hosts in a record (column 16- lines 26-45).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Kaashoek by during a first time interval, comparing (a) identities of destination hosts identified in requests to send data from the first host and (b) identities of destination hosts identified in the record as taught by Barrett in order to prevent the sending of SPAM messages (Barrett- column 16- lines 36-40).

Considering **Claim 2 and 32,** the combination discloses the record is established by monitoring identities of destination hosts to whom requests have been transmitted during a second time interval, which precedes the first time interval (Barrett- column 16- lines 26-45).

Considering **Claims 3 and 31,** the combination discloses the record contains a predetermined maximum number of destination host identities, the maximum number being defined in accordance with a policy (Barrett- column 1- lines 26-57).

Considering **Claim 4 and 33,** the combination discloses the policy additionally defines a maximum number of destination host identities not in the record, to whom requests may be legitimately transmitted in accordance with policy (Barrett- column 1- lines 26-57).

Considering **Claim 5 and 34,** the combination discloses the step, at the end of any given time interval, of deleting from the buffer data relating to requests transmitted during the given time interval in accordance with policy (Kaashoek- Fig. 4).

Considering **Claim 6,** the combination discloses the step, at the end of the given time interval, of updating the record to reflect identities of hosts identified in requests which are transmitted in accordance with policy during the given time interval (Kaashoek- Fig. 4, Barrett- column 16- lines 26-45).

Considering **Claim 7,** the combination discloses the step of updating the record to reflect the identity of the predetermined maximum number of destination host identities to whom data has most recently been sent in accordance with policy (Barrett- column 1- lines 26-57).

Considering **Claim 8,** the combination discloses the stored data is offered in a buffer and includes a copy of a socket created to send data in accordance with a request (Kaashoek- Fig. 4).

Considering **Claims 9 and 30,** the combination discloses the socket enables identification of at least one application program at whose behest the socket is created (Barrett- column 11- lines 30-41).

Considering **Claim 15,** the combination discloses the step of monitoring the rate of increase in the size of the buffer, and in the event that the rate of increase in the size of the buffer exceeds a predetermined rate, generating a warning (Barrett- column 16- lines 26-45).

Considering **Claim 16,** the combination discloses monitoring the increase in the size of the buffer per time interval, and in the event that the increase in the size of the buffer in any given time interval exceeds the predetermined size, generating a warning (Barrett- column 16- lines 26-45).

Considering **Claim 17,** the combination discloses the step of monitoring the size of the buffer, and in the event that the buffer exceeds a predetermined size for a predetermined number of successive time intervals, generating a warning (Barrett- column 16- lines 26-45).

Considering **Claim 18,** the combination discloses at least one parameter selected from the group consisting of: number of destination hosts in the record; threshold number of requests identifying destination hosts not in the record and defining a state of viral infection, is varied with time (Barrett- column 16- lines 26-45).

Considering **Claims 19 and 22,** the combination discloses at least one parameter is varied as a function of the time of day (Barrett- column 16- lines 26-45).

Considering **Claim 20,** the combination discloses at least one of the parameters is varied in response to a perceived threat level (Barrett- column 16- lines 26-45).

Considering **Claim 21,** the combination discloses at least one of the parameters is changed between a first set of values and a second set of values at a predetermined rate (Kaashoek- Fig. 4, Barrett- column 16- lines 26-45).

Considering **Claim 23,** the combination discloses at least one parameter selected from the group consisting of: number of destination hosts in the record; threshold number of requests identifying destination hosts not in the record and defining

a state of viral infection, is determined by performing an automated search on a set of data indicative of normal network traffic (Kaashoek- Fig. 4, Barrett- column 16- lines 26-45).

Considering **Claims 35 and 38,** the combination discloses the step, in the event that the number of socket data items stored exceeds a predetermined value, of storing outgoing packets from the first host (column 4- lines 34-53).

Considering **Claim 36 and 39,** the combination discloses packets having a designated destination IP address is stored (column 4- lines 34-53).

Considering **Claim 37 and 40,** the combination discloses the step of establishing the predetermined IP address from the stored socket data (column 4- lines 34-53).

.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to RANDAL D. MORAN whose telephone number is (571)270-1255. The examiner can normally be reached on M-F: 7:00 - 4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Randal D. Moran/
Examiner, Art Unit 2435

/Kimyen Vu/

Supervisory Patent Examiner, Art Unit 2435